

Please type a plus sign (+) inside this box



Based on PTO/SB/21 (05-03)

Approved for use through 04/30/2003. OMB 0651-0031  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE  
Under the Paperwork Reduction Act of 1995, no persons are required to respond  
to a collection of information unless it displays a valid OMB control number.

AP/IFW  
2134  
\$



<b>TRANSMITTAL FORM</b>  (to be used for all correspondence after initial filing)	Application Number	09/451,575
	Filing Date	11/30/1999
	First Named Inventor	Ho Wing Sit
	Group Art Unit	2134
	Examiner Name	Nalven, Andrew L.
Total Number of Pages in This Submission	Attorney Docket Number	ACCE.P0004

Enclosures (Check all that apply)		
<input type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Assignment Papers (for an application)	<input type="checkbox"/> After Allowance Communication to Group
<input type="checkbox"/> Fee Attached	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input type="checkbox"/> Amendment/Reply	<input type="checkbox"/> Licensing-related Papers	<input checked="" type="checkbox"/> Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declarations(s)	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Status Letter
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address	<input checked="" type="checkbox"/> Other Enclosures (Listed below): <b>Postcard</b> <b>Credit Card Payment Form</b>
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Terminal Disclaimer	
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Certified Copy of Priority Documents	<input type="checkbox"/> CD, Number of CD(s) _____	
<input type="checkbox"/> Response to Missing Parts/Incomplete Application	<b>Remarks:</b>	
<input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm Or Individual name	John Stattler, Reg. No. 36,285 of Stattler Johansen & Adeli LLP
Signature	
Date	August 3, 2004

CERTIFICATE OF TRANSMISSION/MAILING			
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Services as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date: 8/3/04			
Typed or printed name	John Stattler		
Signature		Date	August 3, 2004

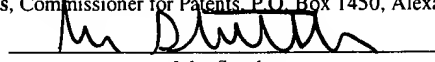
This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**



PATENT  
Docket No. ACCE.P0004

**CERTIFICATE OF MAILING BY "FIRST CLASS MAIL"**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: **Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on August 3, 2004.**

  
John Stattler

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Patent Application for:

Ho Wing SIT; Tony F. KINNIS

Serial No.: 09/451,575

Filing Date: November 30, 1999

For: INTEGRATING A DIGITAL  
SIGNATURE SERVICE INTO A  
DATABASE

Examiner: Andrew L. NALVEN

Group Art Unit: 2134

**APPEAL BRIEF**

Mail Stop Appeal Brief-Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This is an Appeal from the final rejection of claims 1-21 in the above-referenced application. In accordance with 37 C.F.R. § 1.192, this Brief, along with the accompanying Appendix, is filed in triplicate and is accompanied by the required fee. Please charge any additional fees or credit any overpayment to Deposit Account No. 501128, referencing ACCE.P0004.

**I. REAL PARTY IN INTEREST**

The real party in interest to this Appeal is Accela, Inc., a California Corporation, having its principal place of business in Dublin, California.

08/09/2004 WARDELRI 00000021 09451575

01 FC:2402

165.00 OP

Customer No.: 23329  
VPT

Page 1 of 21

Reference No.: ACCE.P0004  
PTO Serial Number: 09/451,575

## **II. RELATED APPEALS AND INTERFERENCES**

There are no related appeals or interferences known to Applicant, Applicant's legal representative, or assignees thereof.

## **III. STATUS OF CLAIMS**

Claims 1-21 are pending in the present application. The Examiner has rejected claims 1-21. Applicants hereby appeal the rejection of claims 1-21.

## **IV. STATUS OF AMENDMENTS**

No amendments to the application were submitted after final rejection.

## **V. SUMMARY OF INVENTION**

A digital signature service is integrated into a database. (*Specification*, page 3, lines 12)  
A client of the database, such as an application program, generates a command to the RDBMS [database] to execute a stored procedure or stored function. (*Specification*, page 4, lines 2-4)  
The store procedure works towards digitally signing the data and saving the data in a persistent datastore. (*Specification*, page 4, lines 2-4) In response to the store procedure, a digital certificate and a private key of the client are received, (*Specification*, page 4, lines 4-5), a signature is generated from data, the digital certificate, and the private key is generated, (*Specification*, page 4, lines 5-6), a signature object is generated from the signature, data, and the digital certificate, (*Specification*, page 4, lines 6-7), and the signature object is stored in a record of the database. (*Specification*, page 4, lines 7-8)

## **VI. ISSUES**

I. Are claims 1-2, 5-6, 11-12, 15-16 and 21 anticipated under 35 U.S.C. § 102(e) by Bisbee (US Patent 6,237,096)?

II. Are claims 3-4 and 13-14 unpatentable under 35 U.S.C. § 103(a) over Bisbee (US Patent 6,237,096) in view of Date ("An Introduction to database Systems", by C. J. Date)?

III. Are claims 9-10 and 19-20 unpatentable under 35 U.S.C. § 103(a) over Bisbee (US Patent 6,237,096) in view of Applicant's Claimed Invention?

IV. Are claims 7-8 and 17-18 unpatentable under 35 U.S.C. § 103(a) over Bisbee (US Patent 6,237,096) in view of Ramasubramani (US Patent 6,233,577)?

## VII. GROUPING OF CLAIMS

As grouped by the Examiner through each ground of rejection, Applicant states that the claims of such grouping do not stand or fall together. The separately patentable claims are grouped as follows:

Group I: Claims 1 and 11 and claims 5, 7-8, 15, 17-18, and 21, which fall therewith;

Group II: Claims 2 and 12;

Group III: Claims 3 and 13;

Group IV: Claims 4 and 14;

Group V: Claims 6 and 16; and

Group VI: Claims 9 and 19 and claims 10 and 20, which fall therewith.

## VI. ARGUMENT

### I. CLAIMS 1-2, 5-6, 11-12, 15-16 AND 21 ARE NOT ANTICIPATED UNDER 35 U.S.C. § 102(E) BY BISBEE (US PATENT 6,237,096)

The Examiner rejected claims 1-2, 5-6, 11-12, 15-16 and 21 as anticipated under 35 U.S.C. § 102(e) by Bisbee (US Patent 6,237,096).

Anticipation under 35 U.S.C. Section 102(e) requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros., Inc. v. Union Oil Co., 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) (citing Structural Rubber Prods. Co. v. Park Rubber Co., 749 F.2d 707, 715, 223 USPQ 1264, 1270 (Fed. Cir. 1984); Connell v. Sears, Roebuck & Co., 722 F.2d 1542, 1548, 220

USPQ 193, 198 (Fed. Cir. 1983); Kalman v. Kimberly-Clark Corp., 713 F.2d 760, 771, 218 USPQ 781, 789 (Fed. Cir. 1983)). "[A]bsence from the reference of any claimed element negates anticipation." Kloster Speedsteel AB v. Crucible, Inc., 793 F.2d 1565, 1571, 230 USPQ 81, 84 (Fed. Cir. 1986).

**A. Claim 1 and claim 11 are independent claims.**

**Claim 1** and **claim 11** recite storing a database comprising a plurality of records. The examiner cites the database of the Bisbee's Authentication Center as teaching the claimed database. (03/03/2004 Office Action, Page 3, lines 8-9).

**Claim 1** and **claim 11** recite receiving a store procedure with data from a client of said database. The examiner cites Bisbee's Transfer Agent as teaching the claimed client of the database. (03/03/2004 Office Action, Page 3, line 16) Since Bisbee teaches that a user of the Transfer Agent is a client of the Authentication Center and not of the Authentication Center's database, the above limitation is absent from Bisbee.

**Claim 1** and **claim 11** recite receiving a store procedure with data from a client of said database. Page 4, lines 2-4 of Applicant's specification explains "Specifically, the database client generates a command to the RDBMS [database] to execute a stored procedure or stored function that digitally signs the data and that saves the data in a persistent datastore." There is nothing within Bisbee that teaches the above limitation.

On page 4, item 7 of the Office Action, the Examiner states "Examiner has interpreted Bisbee's process of creating a document, transferring the client signed document to the authentication center (database), and subsequent storage (Bisbee, Figure 7) as the claimed "store procedure." However, "creating," transferring," and "storing" are implementations of commands and not commands in and of themselves. Thus, the Examiner failed to establish that Bisbee teaches the above limitation.

Bisbee teaches at col. 7, lines 5-8 that "the authenticated, digitally signed and/or encrypted documents are stored by the third-party Authentication Center." Such storage is not the result of a command received by Bisbee's Authentication Center from Bisbee's Transfer Agent but rather the result of procedures already stored in Bisbee's Authentication Center. This makes sense for the non-repudiation portion of Bisbee's invention.

For non-repudiation (preventing the originator of a document from denying the document's originator Bisbee, col. 3, lines 3-4), Bisbee teaches that original authenticated electronic documents stored in the Authentication Center provide irrefutable proof when a transfer of ownership takes place. (Bisbee, col. 12, lines 32-38). Since Bisbee teaches that the originator of an accepted offer document may send that document directly to the Authentication Center (Bisbee, col. 13, lines 3-5), it would not make sense in view of Bisbee's non-repudiation teaching for Bisbee to teach that the originator of an accepted offer document (Transfer Agent) may also control whether the Authentication Center stores her original authenticated electronic document in the Authentication Center. As the Examiner notes in the Office Action, page 5, item 12, lines 9-10, Bisbee teaches that the authenticated information objects are stored under the control of the Authentication Center (trusted repository) rather than by receiving a store procedure from the Transfer Agent.

Accordingly, the above limitation is absent from Bisbee.

**Claim 1** and **claim 11** recite receiving a store procedure with data ... in response to said store procedure, receiving a digital certificate for said client; receiving a private key for said client; generating a signature from said data, digital certificate and private key of said client.

The examiner cites Bisbee's Transfer Agent as teaching the claimed client of the database. (03/03/2004 Office Action, Page 3, line 16) Bisbee teaches moving the heart of the cryptographic process to a Token entrusted to a respective authorized Transfer Agent (client).

(Bisbee, col. 7, lines 39-41). Once a signature is generated from data, Bisbee teaches that the Authentication Center receives the digitally signed version of a digital document from the Transfer Agent's Token. (Bisbee, col. 6, lines 46, 51-54). Rather than using a private key of the Transfer Agent client or the digital certificate of the client, the Authentication Center of Bisbee makes use of its own secret key to sign again the transaction. (Bisbee, col. 8, lines 15-16). Thus, Bisbee does not teach generating a signature from said data, digital certificate and private key of said client.

The Examiner cites Bisbee, col. 11, lines 15-20, Fig. 8 as teaching the above limitation. However, the cited text is not in response to a store procedure and is not performed by Bisbee's Authentication Center. As noted above, rather than using a private key of the Transfer Agent client or the digital certificate of the client, the Authentication Center of Bisbee makes use of its own secret key to sign again the transaction. Bisbee, col. 8, lines 15-16, col. 11, lines 40-42.

Thus, the above limitation is absent from Bisbee.

**Claim 1** and **claim 11** recite receiving a store procedure with data ... in response to said store procedure, ... generating a signature object for said data, said digital signature object comprising said data, certificate and signature.

The Authentication Center of Bisbee does not perform this step. Thus, The above limitation is absent from Bisbee.

**Claim 1** and **claim 11** recite receiving a store procedure with data ... in response to said store procedure, ... storing said signature object as at least a portion of one of said records in said database.

Since Bisbee does not teach "receiving a store procedure with data from a client of said database," the above limitation is absent from Bisbee as well.

**B. Claim 2 depends from independent claim 1 and claim 12 depends from independent claim 11.**

**Claim 2** and **claim 12** recite: retrieving, in response to said query command, said data, certificate and signature for said user; ... processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents.

The Examiner cites Bisbee col. 11, lines 28-40 as teaching this limitation. Bisbee's teaching at col. 11, lines 28-40 is not in response to a query command. Thus, the above limitation is absent from Bisbee.

**C. Claim 6 depends from claim 5 and claim 16 depends from claim 15.**

**Claim 6** and **claim 16** recite: wherein the step of generating a single signature object comprises the step of generating a serialized object comprising said certificate, said document, and said signature. Page 18, lines 1-4 of Applicant's specification explains "Since the information is written to a file as serialized objects, an attempt to intercept the file to replace it with extraneous data would be difficult because the intruder would have to extract the information in exactly the same fashion as it was written to the file."

The Examiner cites Bisbee FIG. 9 as teaching the above limitation. There is nothing within FIG. 9 to indicate that the certificate, document, and signature need to be extracted in exactly the same fashion as it was written to the file. Thus, there is nothing within FIG. 9 to indicate that certificate, document, and signature of FIG. 9 are a serialized object.

Accordingly, the above limitation is absent from Bisbee.

**D. Claim 21 is independent.**

**Claim 21** recites: database client for generating a store procedure with data.

For the reasons noted above, Bisbee does not teach this limitation.



**Claim 21** recites: database management system, coupled to said database client, for generating, in response to said store procedure, a signature from said data, said database management system further for generating a signature object for said data, digital certificate and private key of said database client, said digital signature object comprising said data, certificate and signature.

For the reasons noted above, the above limitation is absent from Bisbee.

**E. Conclusion**

The absence of the above showings negates anticipation. Therefore, the Board should reverse the anticipation rejection of claim 1 and claims 5-6, 11, which fall therewith; of claim 8 and claims 9-11, which fall therewith; and of claim 14 and claims 16 and 18, which fall therewith.

**II. CLAIMS 3-4 AND 13-14 ARE NOT RENDERED OBVIOUS, UNDER 35 U.S.C. § 103, OVER BISBEE IN VIEW OF DATE.**

The Examiner rejected claims 3-4 and 13-14 as unpatentable under 35 U.S.C. § 103(a) over Bisbee (US Patent 6,237,096) in view of Date ("An Introduction to database Systems", by C. J. Date).

It is well established that the Examiner has this burden of establishing a *prima facie* case for obviousness. In re Fine, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988). Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching, suggestion or incentive supporting the combination. In re Geiger, 2 U.S.P.Q.2d 1276, 1278 (Fed. Cir. 1987).

To establish a *prima facie* case of obviousness, the Examiner must establish three basic criteria. First, the prior art reference (or references when combined) must teach or suggest all the claim limitations. Second, there must be some suggestion or motivation in the references

themselves to modify the reference or to combine reference teachings. Finally, there must be a reasonable expectation of success. MPEP 2143.

"In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness." In re Rijckaert, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993)(citing In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992)). "A prima facie case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art." In re Bell, 991 F.2d 781, 783, 26 USPQ2d 1529, 1531 (Fed. Cir. 1993) (quoting In re Rinehart, 531 F.2d 1048, 1051, 189 USPQ 143, 147 (CCPA 1976)).

**A. BISBEE AND DATE DO NOT TEACH OR SUGGEST ALL THE CLAIM LIMITATIONS.**

**Claim 3** and **claim 13** recite receiving, as said query command, a query command to retrieve at least one record in said database comprising criteria based on digital signatures stored for said records.

Neither cited references teaches or suggests the above limitation.

It is well known that "Obviousness may not be established using hindsight or in view of the teachings or suggestions of the inventor." Para-Ordnance Manufacturing, Inc. v. SGS Importers International, Inc., 73 F.3d 1085, 1087, 37 USPQ2d 1237, 1239 (Fed. Cir. 1995). The examiner asserts that Date teaches the above limitation since (i) Date teaches "that databases can be queried by using row or column sub-setting operation" (03/03/2004 Office Action, Page 7, lines 4-5) and (ii) Applicant's disclosure teaches "a database table comprising a document, signature, and certificate may be searched for records containing a specific signature." (03/03/2004 Office Action, Page 7, lines 7-9). Since the Examiner impermissibly used

Applicant's teachings to establish obviousness, the Examiner failed to make out a prima facie case of obviousness.

**Claim 4 and claim 14** recite processing said data and said certificate (from queried, received, and extracted records), using said signature, to verify that said data and said certificate are unaltered from their original contents.

Neither cited references teaches or suggests the above limitation.

Here, the examiner fails to allege, let alone show, that the addition of Date cures the deficiency of Bisbee. Absent a teaching or suggestion that a method processes data and a certificate queried, received, and extracted as claimed, the examiner fails to present a prima facie case of obviousness.

**B. NEITHER BISBEE NOR DATE PROVIDE A MOTIVATION TO COMBINE THE REFERENCE TEACHINGS.**

The examiner states that the motivation to combine Bisbee and Date is that such a combination would allow the user to find all documents created by the same signatory or signed by the same digital signature. (03/03/2004 Office Action, Page 7, lines 11-12). Since this motivation is not in the reference teachings, the Examiner failed to make out a prima facie case of obviousness.

Date teaches basic database concepts. Date does not mention or suggest using a digital signature service in conjunction with a database store procedure. In order to render a combination obvious, there must be some suggestion to combine the teachings. Neither Bisbee nor Date provides a suggestion to combine the teaching of Date's database with Bisbee's Authentication Center.

C. CONCLUSION

In view of the above, the Board should reverse the obviousness rejection of claims 3-4 and 13-14.

III. CLAIMS 9-10 AND 19-20 ARE NOT RENDERED OBVIOUS, UNDER 35 U.S.C. § 103, OVER BISBEE IN VIEW OF APPLICANT'S CLAIMED INVENTION.

The Examiner rejected claims 9-10 and 13-14 as unpatentable under 35 U.S.C. § 103(a) over Bisbee (US Patent 6,237,096) in view of Applicant's Claimed Invention.

A. BISBEE AND DATE DO NOT TEACH OR SUGGEST ALL THE CLAIM LIMITATIONS.

**Claim 9** and **claim 19** recite *generating a second signature object, said second signature object comprising said first signature object, said second certificate, and said second signature.*

Bisbee does not teach or suggest the above limitation. The Examiner acknowledges this by stating "Bisbee's disclosure ... lacks reference to a second certificate and signature from a second source being used to create a second signature object." (03/03/2004 Office Action, Page 7, lines 15-16 (Item 18))

It is well known that "Obviousness may not be established using hindsight or in view of the teachings or suggestions of the inventor." Para-Ordnance Manufacturing, Inc. v. SGS Importers International, Inc., 73 F.3d 1085, 1087, 37 USPQ2d 1237, 1239 (Fed. Cir. 1995). The examiner asserts that "applying a certificate and a signature to a first signature object as defined by the claims" would generate the claimed second signature object. (03/03/2004 Office Action, Page 7, lines 18-19). Since the Examiner impermissibly used Applicant's teachings to establish obviousness, the Examiner failed to make out a prima facie case of obviousness.

**B. THE EXAMINER ERRED BY USING APPLICANTS' DISCLOSURE TO DEMONSTRATE MOTIVATION TO COMBINE.**

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure." MPEP 2143.

The examiner states that the motivation to combine Bisbee and Applicant's Claimed Invention is that such a combination would add additional protection measures to the document. (03/03/2004 Office Action, Page 7, line 22; page 8, line 1). As stated in Applicant's specification on page 21, lines 23-25, "User 2, through the digital signature service database retrieval procedure 940, verifies the authenticity of user 1 as well as the contents of the document 930 and certificate "1" 935." Since the Examiner found the suggestion to make the claimed combination in Applicant's disclosure, the Examiner failed to make out a prima facie case of obviousness.

**C. CONCLUSION**

In view of the above, the Board should reverse the obviousness rejection of claims 9-10 and 19-20.

**IV CLAIMS 7-8 AND 17-18 ARE NOT RENDERED OBVIOUS, UNDER 35 U.S.C. § 103, OVER BISBEE IN VIEW OF RAMASUBRAMANI.**

The Examiner rejected claims 7-8 and 17-18 unpatentable under 35 U.S.C. § 103(a) over Bisbee (US Patent 6,237,096) in view of Ramasubramani (US Patent 6,233,577).

**Claim 7** and **claim 8** stand or fall with claim 1. **Claim 17** and **claim 18** stand or fall with claim 11.

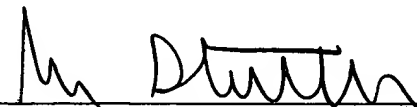
## VII. CONCLUSION.

In view of the foregoing, Applicants respectfully submit that the claims are patentable over the prior art. Applicants hereby request that the Board overturn the Examiner's finding that the claims are anticipated and /or rendered obvious in view of the cited references.

Dated: August 3, 2004

Respectfully submitted,  
STATTLER JOHANSEN & ADELI LLP

Stattler, Johansen & Adeli LLP PO Box 51860 Palo Alto, California 94303-0728 Telephone: (650) 752-0990 Facsimile: (650) 752-0995
----------------------------------------------------------------------------------------------------------------------------------------------

By:   
John C. Stattler  
Registration No. 36,285  
Direct Phone No.: (650) 752-0990, x100

## **APPENDIX**

### **The following claims are involved in this Appeal:**

1. A method for integrating a digital signature service into a database, said method comprising the steps of:

storing a database comprising a plurality of records;

receiving a store procedure with data from a client of said database;

in response to said store procedure,

receiving a digital certificate for said client;

receiving a private key for said client;

generating a signature from said data, digital certificate and private key of said client;

generating a signature object for said data, said digital signature object comprising said data, certificate and signature; and

storing said signature object as at least a portion of one of said records in said database.

2. The method as set forth in claim 1, further comprising the steps of:

receiving a query command from said user to retrieve said data from said record of said database table;

retrieving, in response to said query command, said data, certificate and signature for said user;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents;

obtaining, from said certificate, an authentication as to the digital signatory; and

generating, as a response to said query command, said data, so as to provide verification of said data with said signature and said certificate in response to said query.

3. The method as set forth in claim 2, further comprising the steps of:

receiving, as said query command, a query command to retrieve at least one record in said database comprising criteria based on digital signatures stored for said records;

identifying records in said database with said criteria regarding said digital signatures;

and

retrieving said records identified in response to said query command.

4. The method as set forth in claim 3, further comprising the steps of:

extracting, from said records retrieved, data, certificate and signature stored in said record;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents;

obtaining, from said certificate, an authentication as to the digital signatory of said data;

and

generating, as a response to said query command, said data, so as to provide verification of said data with said signature and said certificate in response to said query.

5. The method as set forth in claim 1, wherein:

the step of generating a digital signature for said data comprises the step of generating a single signature object comprising said certificate, said document, and said digital signature; and



the step of storing said document, certificate and signature as at least a portion of a record in said database comprises the step of storing said single signature object in said record of said database.

6. The method as set forth in claim 5, wherein the step of generating a single signature object comprises the step of generating a serialized object comprising said certificate, said document, and said signature.

7. The method as set forth in claim 1, further comprising the step of storing said certificate of said user in a column of said database table.

8. The method as set forth in claim 7, wherein the step of storing said certificate of said user in a column of said database table comprises the step of augmenting a user identification field to include said certificate of said user.

9. The method as set forth in claim 1, further comprising the steps of:

- receiving a second digital certificate for a second client;
- retrieving said signature object from said record in said database as a first signature object;
- generating a second signature from said first signature object with said second client as a signatory;
- generating a second signature object, said second signature object comprising said first signature object, said second certificate, and said second signature; and
- storing, in said database, said second signature object.

10. The method as set forth in claim 9, further comprising the steps of:

receiving a query command to retrieve said second signature object from said record of said database table;

retrieving, in response to said query command, said second signature object for said user;

processing said first signature object and said second certificate, using said second signature, to verify that said first signature object and said second certificate are unaltered from their original contents;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents; and

generating, as a response to said query command, said data, so as to provide verification of said first and second digital signatures.

11. A computer readable medium comprising a plurality of instructions which, when executed by a computer, cause the computer to perform the steps of:

storing a database comprising a plurality of records;

receiving a store procedure with data from a client of said database;

in response to said store procedure,

receiving a digital certificate for said client;

receiving a private key for said client;

generating a signature from said data, digital certificate and private key of said client;

generating a signature object for said data, said digital signature object comprising said data, certificate and signature; and

storing said signature object as at least a portion of one of said records in said database.

12. The computer readable medium as set forth in claim 11, further comprising the steps of:

receiving a query command from said user to retrieve said data from said record of said database table;

retrieving, in response to said query command, said data, certificate and signature for said user;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents;

obtaining, from said certificate, an authentication as to the digital signatory; and

generating, as a response to said query command, said data, so as to provide verification of said data with said signature and said certificate in response to said query.

13. The computer readable medium as set forth in claim 12, further comprising the steps of:

receiving, as said query command, a query command to retrieve at least one record in said database comprising criteria based on digital signatures stored for said records;

identifying records in said database with said criteria regarding said digital signatures;

and

retrieving said records identified in response to said query command.

14. The computer readable medium as set forth in claim 13, further comprising the steps of:

extracting, from said records retrieved, data, certificate and signature stored in said record;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents;

obtaining, from said certificate, an authentication as to the digital signatory of said data; and

generating, as a response to said query command, said data, so as to provide verification of said data with said signature and said certificate in response to said query.

15. The computer readable medium as set forth in claim 11, wherein:

the step of generating a digital signature for said data comprises the step of generating a single signature object comprising said certificate, said document, and said digital signature; and

the step of storing said document, certificate and signature as at least a portion of a record in said database comprises the step of storing said single signature object in said record of said database.

16. The computer readable medium as set forth in claim 15, wherein the step of generating a single signature object comprises the step of generating a serialized object comprising said certificate, said document, and said signature.

17. The computer readable medium as set forth in claim 11, further comprising the step of storing said certificate of said user in a column of said database table.

18. The computer readable medium as set forth in claim 17, wherein the step of storing said certificate of said user in a column of said database table comprises the step of augmenting a user identification field to include said certificate of said user.

19. The computer readable medium as set forth in claim 11, further comprising the steps of:

receiving a second digital certificate for a second client;

retrieving said signature object from said record in said database as a first signature object;

generating a second signature from said first signature object with said second client as a signatory;

generating a second signature object, said second signature object comprising said first signature object, said second certificate, and said second signature; and

storing, in said database, said second signature object.

20. The computer readable medium as set forth in claim 19, further comprising the steps of:

receiving a query command to retrieve said second signature object from said record of said database table;

retrieving, in response to said query command, said second signature object for said user;

processing said first signature object and said second certificate, using said second signature, to verify that said first signature object and said second certificate are unaltered from their original contents;

processing said data and said certificate, using said signature, to verify that said data and said certificate are unaltered from their original contents; and

generating, as a response to said query command, said data, so as to provide verification of said first and second digital signatures.

21. A computer comprising:

an input device for receiving a digital certificate and a private key for a user of said computer;

database client for generating a store procedure with data ;

database management system, coupled to said database client, for generating, in response to said store procedure, a signature from said data, said database management system further for generating a signature object for said data, digital certificate and private key of said database client, said digital signature object comprising said data, certificate and signature; and

database, coupled to said database management system, comprising a plurality of records for storing said signature object as at least a portion of a record.